

WHAT IS CLAIMED IS:

- 1 1. A method for authorizing a customer to perform transactions with a
2 self-service device, the method comprising:
3 extracting a first set of biometric data regarding the customer from a
4 verification instrument;
5 extracting a second set of biometric data directly from at least one feature of
6 the customer;
7 extracting textual data regarding the customer from the verification
8 instrument;
9 comparing the first and second sets of biometric data to determine whether the
10 first and second sets of biometric data are derived from a single individual; and
11 recording customer identification information if it is determined that the first
12 and second sets of biometric data are derived from the customer.
- 1 2. The method recited in claim 1 wherein the customer identification
2 information comprises information derived from the extracted textual data.
- 1 3. The method recited in claim 1 wherein the customer identification
2 comprises a name of the customer.
- 1 4. The method recited in claim 3 wherein the transactions comprise
2 providing funds in exchange for a financial instrument identifying the name of the customer.
- 1 5. The method recited in claim 4 wherein the financial instrument is
2 selected from the group consisting of a note, a draft, a check, and a promissory note.
- 1 6. The method recited in claim 1 wherein the transactions comprise a
2 financial transaction.
- 1 7. The method recited in claim 1 wherein the transactions comprise a
2 nonfinancial transaction.
- 1 8. The method recited in claim 1 wherein the customer identification
2 information comprises a signature of the customer.

1 9. The method recited in claim 1 wherein the customer identification
2 information is further derived from one of the first and second sets of biometric data.

1 10. The method recited in claim 1 wherein the first set of biometric data is
2 derived from image data on the verification instrument.

1 11. The method recited in claim 1 wherein the first set of biometric data is
2 derived from data encoded magnetically on the verification instrument.

1 12. The method recited in claim 1 wherein the first set of biometric data is
2 derived from data encoded optically on the verification instrument.

1 13. The method recited in claim 1 wherein the first and second sets of
2 biometric data are derived from facial features.

1 14. The method recited in claim 1 wherein the first and second sets of
2 biometric data are derived from fingerprints.

1 15. The method recited in claim 1 wherein the first and second sets of
2 biometric data are derived from voice features.

1 16. The method recited in claim 1 wherein the textual data are derived
2 from data encoded magnetically on the verification instrument.

1 17. The method recited in claim 1 wherein the textual data are derived
2 from data encoded optically on the verification instrument.

1 18. The method recited in claim 1 wherein extracting textual data
2 regarding the customer from the verification instrument comprises:
3 extracting a database reference number from the verification instrument; and
4 retrieving the textual data regarding the customer from a database with the
5 database reference number.

1 19. The method recited in claim 18 further comprising prompting the
2 customer to enter data for comparison with the retrieved textual data.

1 20. The method recited in claim 1 wherein the self-service device
2 comprises a self-service kiosk.

1 21. The method recited in claim 1 wherein the self-service device
2 comprises a personal computer.

1 22. The method recited in claim 1 wherein the self-service device
2 comprises a personal digital assistant.

1 23. A method for authorizing a customer to perform transactions with a
2 self-service device, the method comprising:

3 extracting a first set of image data regarding the customer from a verification
4 instrument;

5 extracting a second set of image data directly from at least one feature of the
6 customer;

7 extracting textual data regarding the customer from the verification
8 instrument;

9 comparing the first and second sets of image data to determine whether the
10 first and second sets of image data are derived from a single individual; and

11 recording customer identification information if it is determined that the first
12 and second sets of image data are derived from the customer.

1 24. The method recited in claim 23 wherein the customer identification
2 information comprises information derived from the extracted textual data.

1 25. The method recited in claim 23 wherein comparing the first and second
2 sets of image data comprises having a human examine the first and second sets of image data.

1 26. The method recited in claim 23 wherein the customer identification
2 information is further derived from one of the first and second sets of image data.

1 27. The method recited in claim 23 wherein the textual data are derived
2 from data encoded magnetically on the verification instrument.

1 28. The method recited in claim 23 wherein the textual data are derived
2 from data encoded optically on the verification instrument.

1 29. The method recited in claim 23 wherein the transactions comprise a
2 financial transaction.

1 30. The method recited in claim 23 wherein the transactions comprise a
2 nonfinancial transaction.

1 31. The method recited in claim 23 wherein extracting textual data
2 regarding the customer from the verification instrument comprises:
3 extracting a database reference number from the verification instrument; and
4 retrieving the textual data regarding the customer from a database with the
5 database reference number.

1 32. A method for executing a transaction with a customer, the method
2 comprising:
3 extracting a first set of biometric data directly from at least one feature of the
4 customer;
5 comparing the first set of biometric data with a stored set of biometric data,
6 wherein the stored set of biometric data has previously been authenticated by comparison
7 between a set of biometric data extracted from a verification instrument and a second set of
8 biometric data extracted directly from at least one feature of the customer; and
9 thereafter, completing the transaction if it is determined that the first and
10 stored sets of biometric data are derived from the customer.

1 33. The method recited in claim 32 wherein the transaction comprises a
2 financial transaction.

1 34. The method recited in claim 33 further comprising:
2 extracting textual data from a financial instrument presented by the customer
3 as part of the financial transaction; and
4 comparing the textual data with stored textual data, wherein the stored textual
5 data was extracted from the verification instrument.

1 35. The method recited in claim 34 wherein the textual data comprises a
2 signature of the customer.

1 36. The method recited in claim 34 wherein the textual data comprises a
2 name of the customer.

0950207470550

1 37. The method recited in claim 32 wherein the set of biometric data
2 extracted from the verification instrument is derived from image data on the verification
3 instrument.

1 38. The method recited in claim 32 wherein the set of biometric data
2 extracted from the verification instrument is derived from data encoded magnetically on the
3 verification instrument.

1 39. The method recited in claim 32 wherein the set of biometric data
2 extracted from the verification instrument is derived from data encoded optically on the
3 verification instrument.

1 40. A self-service transaction system comprising:
2 a plurality of networked self-service devices, at least one of the self-service
3 devices including:
4 a first identification device adapted to extract a first set of
5 identification data directly from a customer; and
6 a second identification device adapted to extract a second set of
7 identification data and textual regarding the customer from a verification instrument; and
8 a storage device in communication with the at least one of the self-service
9 devices for storing customer identification information derived from the textual data.

1 41. The system recited in claim 40 further comprising a comparator in
2 communication with the at least one of the self-service devices, the comparator being
3 configured to compare the first and second sets of identification data to determine whether
4 the first and second sets of identification data are derived from a single individual.

1 42. The system recited in claim 41 wherein the comparator is local to the
2 at least one of the self-service devices.

1 43. The system recited in claim 41 wherein the comparator is networked
2 with the plurality of self-service devices.

1 44. The system recited in claim 40 wherein the first and second sets of
2 identification data comprise biometric data.

1 45. The system recited in claim 40 wherein the first and second sets of
2 identification data comprise image data.

1 46. A self-service transaction system comprising:
2 a plurality of networked self-service devices, at least one of the self-service
3 devices including:
4 means for extracting a first set of identification data directly from a
5 customer; and
6 means for extracting a second set of identification data and textual data
7 regarding the customer from a verification instrument;
8 means for comparing the first and second sets of identification data to
9 determine whether the first and second sets of identification data are derived from a single
10 individual; and
11 means for recording customer identification information derived from the
12 textual data.

1 47. The system recited in claim 46 wherein the first and second sets of
2 identification data comprise biometric data.

1 48. The system recited in claim 46 wherein the first and second sets of
2 identification data comprise image data.